ABSTRACT

A method and system is directed to providing policies for handling authenticated messages, such as email, and the like, by combining Public Key encryption and the Internet Domain Name System (the "DNS"). The policies include system, user, statistics, new domain, unverified domain, and third party. A domain owner may validate that an email originates from an authorized sender within their domain by using a private key component to digitally sign email outbound from its domain. Employing a public key component, along with a selector, an email recipient may check the validity of the signature, and thus determine that the email originated from a sender authorized by the domain owner. In one embodiment, the public key component used to verify an email signature may be "advertised" or otherwise made available via a TXT record in the DNS.

Customer No.: 38880